

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-293102

(43)Date of publication of application : 20.10.2000

(51)Int.CL

G09C 1/00  
G06F 12/14  
G06T 7/00

(21)Application number : 11-095268

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 01.04.1999

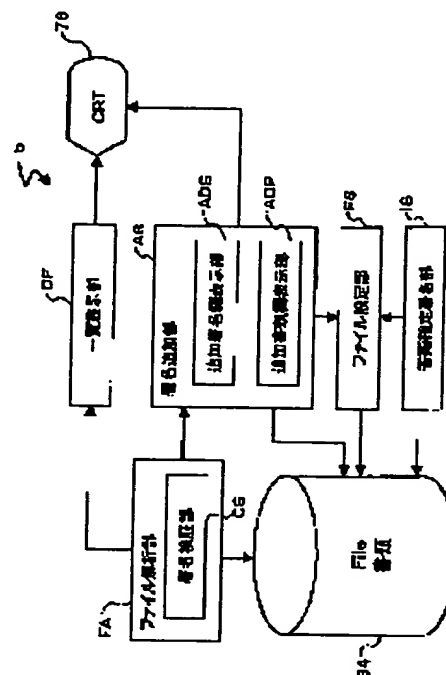
(72)Inventor : KUMAGAI HIDEMITSU

**(54) DIGITAL MULTIPLE SIGNATURE DEVICE AND STORAGE MEDIUM**

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To easily confirm digital signatures and documents and to simply add new digital signatures and new documents.

**SOLUTION:** In a digital multiple signature device 5, when a file, which includes plural digital signatures and documents, is specified, a file analysis section FA analyzes the relationship of the digital signatures and the documents included in the specified file. A summary display section DF displays the analyzed results on a color CRT 76 as a summary. Thus, and operator easily confirms the relationship between each signature and each document. Moreover, a signature adding section AS adds new digital signatures and documents in accordance with the instruction of the operator. When documents and digital signatures are added, a file setting section FS sets all contents including the above into one file and writes the file into a hard disk 84. As a result, new digital signatures and documents are easily added.



## LEGAL STATUS

[Date of request for examination]

**19.02.2001**

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

**[Date of requesting appeal against examiner's decision of rejection]**

[Date of extinction of right]

**This Page Blank (uspto)**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-293102

(F2000-293102A)

(43) 公開日 平成12年10月20日 (2000. 10. 20)

(51) Int.Cl.	識別記号	F I	テーム* (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 B 0 1 7
	6 6 0		6 6 0 D 5 J 1 0 4
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 A 9 A 0 0 1
G 0 6 T 7/00		15/62	4 6 5 P

審査請求 未請求 請求項の数 8 O L (全 16 頁)

(21) 出願番号 特願平11-95268

(22) 出願日 平成11年4月1日 (1999. 4. 1)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 熊谷 秀光

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(74) 代理人 100075258

弁理士 吉田 研二 (外2名)

Fターム(参考) 5B017 AA01 AA04 BA05 BA09 BB03

CA07 CA16

5J104 AA09 LA03 LA07 NA27

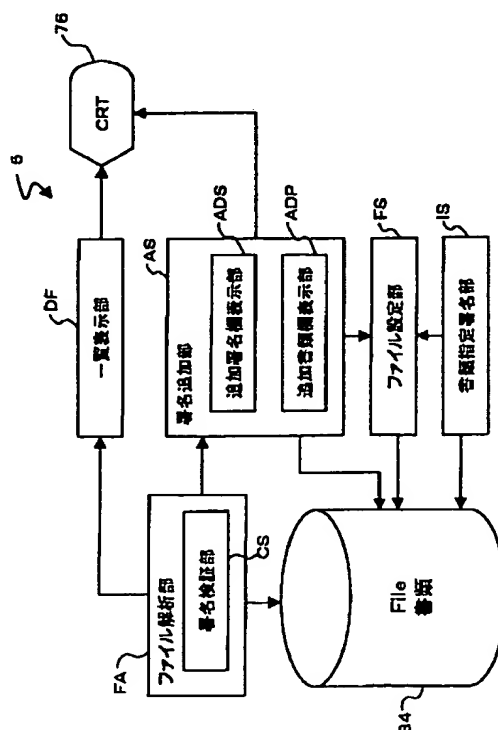
9A001 LL03

(54) 【発明の名称】 デジタル多重署名装置および記憶媒体

(57) 【要約】

【課題】 一目で各デジタル署名と各書類とを確認すると共に新たなデジタル署名や書類を簡単に追加する。

【解決手段】 デジタル多重署名装置 5 では、デジタル署名や書類を複数含むファイルを指定すると、ファイル解析部 F A が指定されたファイルに含まれるデジタル署名や書類の関係を解析し、この解析した結果を一覧表示部 D F が一覧表示としてカラー C R T 7 6 に表示する。したがって、操作者は各デジタル署名と各書類との関係を一目で確認することができる。また、署名追加部 A S は、操作者の指示により新たなデジタル署名や書類を追加する。ファイル設定部 F S は、書類やデジタル署名が追加されると、これらを含むすべての内容を一つのファイルとして設定してハードディスク 8 4 に書き込む。この結果、容易に新たなデジタル署名や書類を追加することができる。



## 【特許請求の範囲】

【請求項1】 少なくとも一つの書類に対して複数のデジタル署名が可能なデジタル多重署名装置であって、指定されたファイルに含まれる書類とデジタル署名との関係を解析するファイル解析手段と、該解析された関係を一覧表示する一覧表示手段と、該一覧表示された関係に対して新たなデジタル署名を追加可能な署名追加手段と、該新たなデジタル署名が追加されたとき、該追加されたデジタル署名と前記指定されたファイルに含まれる書類およびデジタル署名とを所定の関係をもって一つのファイルとして設定するファイル設定手段とを備えるデジタル多重署名装置。

【請求項2】 請求項1記載のデジタル多重署名装置であって、前記署名追加手段は、前記一覧表示手段により表示された関係に対して前記所定の関係をもって前記追加するデジタル署名の欄を表示する追加署名欄表示手段を備え、前記一覧表示手段は、前記ファイル設定手段により前記ファイルが設定されたとき、前記一覧表示している関係に対して前記所定の関係をもって追加されたデジタル署名とを一覧表示する手段であるデジタル多重署名装置。

【請求項3】 前記署名追加手段は、前記デジタル署名の追加の前に新たな書類を追加可能な手段であり、前記一覧表示手段により表示された関係に対して前記所定の関係をもって該追加する書類の欄を表示する追加書類欄表示手段を備える請求項2記載のデジタル多重署名装置。

【請求項4】 請求項1記載のデジタル多重署名装置であって、書類の指定と該指定された書類に対するデジタル署名とが可能な書類指定署名手段を備え、前記ファイル設定手段は、前記書類指定署名手段により指定された書類と該指定された書類に対するデジタル署名とを前記所定の関係をもって一つのファイルとして設定する手段であるデジタル多重署名装置。

【請求項5】 前記一覧表示手段により表示された関係に含まれる書類を指定したとき、該指定された書類を表示する書類表示手段を備える請求項1記載のデジタル多重署名装置。

【請求項6】 請求項1記載のデジタル多重署名装置であって、前記署名追加手段は、前記新たなデジタル署名の追加と共に該デジタル署名に対する検証用データを有する書類を追加する手段であり、前記ファイル設定手段は、前記追加されたデジタル署名および前記追加された書類と前記指定されたファイルに含まれる書類およびデジタル署名と所定の関係をもって一つのファイルとして設定する手段であるデジタル多重署名装置。

【請求項7】 請求項6記載のデジタル多重署名装置であって、

前記書類は、該書類の追加と共に追加されたデジタル署名に対する検証用書類を含み、

前記ファイル解析手段は、前記検証用書類に基づいて該検証用書類を含む書類の追加と共に追加されたデジタル署名を検証する署名検証手段を備えるデジタル多重署名装置。

【請求項8】 指定されたファイルに含まれる書類とデジタル署名との関係を解析するファイル解析処理と、該解析された関係を一覧表示する一覧表示処理と、該一覧表示された関係に対して新たなデジタル署名を追加可能な署名追加処理と、該新たなデジタル署名が追加されたとき、該追加されたデジタル署名と前記指定されたファイルに含まれる書類およびデジタル署名とを所定の関係をもって一つのファイルとして設定するファイル設定処理とをコンピュータに実行させるためのプログラムをコンピュータに読み取り可能に記録した記録媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、デジタル多重署名装置および記憶媒体に関し、詳しくは、少なくとも一つの書類に対して複数のデジタル署名が可能なデジタル多重署名装置および少なくとも一つの書類に対して複数のデジタル署名を可能とする処理をコンピュータに実行させるためのプログラムを記憶したコンピュータにより読み取り可能な記憶媒体に関する。

## 【0002】

【従来の技術】官公庁や自治体、民間企業などの組織体の中で取り交わされる契約書などの書類に対して、紙によるやり取りに代えてコンピュータを利用して作成した電子文書によるやり取りをするに当たり、本人性の保証や他者等による改竄の防止のために電子的な署名（デジタル署名）を複数可能とするものが種々提案されており、それらを活用して複数の電子的な署名が可能である。こうした装置では、例えば、次のように書類の作成やデジタル署名、ファイルの授受が行なわれている。まず、一方の組織体が契約書などの書類を作成すると共に、この作成した書類に対してデジタル署名を行なって一つのファイルとし、これを契約などを締結する他の組織体に送付する。次に、このファイルを受け取った他の組織体は、ファイルを開いて書類とデジタル署名とを確認し、新たな書類を追加し、追加した書類を含めてすべてに対してデジタル署名を行なうと共に、新たに行なったデジタル署名を含めてすべてを一つのファイルとする。このファイルでは、新たなデジタル署名は、新たな書類とそれ以前のデジタル署名や書類を階層的に含む構造として一つのファイルとされる。そして、他の組織体は、そのファイルを正本として保存すると共に、そのフ

ファイルの複製を最初に書類を作成した組織体へ送付する。最初に書類を作成した組織体は、受け取った複製のファイルを開いて書類とデジタル署名とを確認し、これを副本として保存する。なお、書類には、デジタル署名の本人性や改竄の防止のための検証用データを有する認定書等が含まれている。

#### 【0003】

【発明が解決しようとする課題】しかしながら、こうした装置では、ファイルの内容、特にデジタル署名の内容をすぐに確認できないという問題があった。複数のデジタル署名を含むファイルは、デジタル署名を重ねる毎に階層構造を深めるように作成されるから、ファイルを指定すると、通常、最後になされたデジタル署名とその際に追加された書類に対して確認可能な操作画面が表示される。それ以前になされたデジタル署名や書類を確認したいときには、操作画面に対して所定の操作を繰り返して階層構造の深い位置まで移行して、所望のデジタル署名や書類を確認可能な操作画面を表示してから行なう。これでは、多数のデジタル署名がなされたファイルを開いてデジタル署名や書類を確認するときには、多くの操作と時間を要してしまう。

【0004】本発明のデジタル多重署名装置は、多くの操作なしに所望のデジタル署名と書類とを確認することを目的の一つとする。また、本発明のデジタル多重署名装置は、簡易に新たなデジタル署名や書類を追加することを目的の一つとする。

【0005】本発明の記憶媒体は、コンピュータを多くの操作なしに所望のデジタル署名と書類とを確認できる装置にすることを目的の一つとする。また、本発明の記憶媒体は、コンピュータを簡易な操作で新たなデジタル署名や書類を追加可能な装置にすることを目的の一つとする。

#### 【0006】

【課題を解決するための手段およびその作用・効果】本発明のデジタル多重署名装置および記憶媒体は、上述の目的の少なくとも一部を達成するために以下の手段を採った。

【0007】本発明のデジタル多重署名装置は、少なくとも一つの書類に対して複数のデジタル署名が可能なデジタル多重署名装置であって、指定されたファイルに含まれる書類とデジタル署名との関係を解析するファイル解析手段と、該解析された関係を一覧表示する一覧表示手段と、該一覧表示された関係に対して新たなデジタル署名を追加可能な署名追加手段と、該新たなデジタル署名が追加されたとき、該追加されたデジタル署名と前記指定されたファイルに含まれる書類およびデジタル署名とを所定の関係をもって一つのファイルとして設定するファイル設定手段とを備えるものである。

【0008】この本発明のデジタル多重署名装置では、一覧表示手段が、ファイル解析手段により解析された指

定されたファイルに含まれる書類とデジタル署名との関係を一覧表示するから、ファイルに含まれる書類とデジタル署名とを容易に確認することができる。また、本発明のデジタル多重署名装置では、署名追加手段により、この一覧表示された関係に対して新たなデジタル署名が追加可能なので、簡易に新たなデジタル署名を追加することができる。

【0009】こうした本発明のデジタル多重署名装置において、前記署名追加手段は前記一覧表示手段により表示された関係に対して前記所定の関係をもって前記追加するデジタル署名の欄を表示する追加署名欄表示手段を備え、前記一覧表示手段は前記ファイル設定手段により前記ファイルが設定されたとき前記一覧表示している関係に対して前記所定の関係をもって追加されたデジタル署名とを一覧表示する手段であるものとすることもできる。こうすれば、新たなデジタル署名の追加を確認しながら行なうことができる。この態様の本発明のデジタル多重署名装置において、前記署名追加手段は、前記デジタル署名の追加の前に新たな書類を追加可能な手段であり、前記一覧表示手段により表示された関係に対して前記所定の関係をもって該追加する書類の欄を表示する追加書類欄表示手段を備えるものとすることもできる。こうすれば、新たな書類をも簡易に追加することができる。

【0010】また、本発明のデジタル多重署名装置において、書類の指定と該指定された書類に対するデジタル署名とが可能な書類指定署名手段を備え、前記ファイル設定手段は前記書類指定署名手段により指定された書類と該指定された書類に対するデジタル署名とを前記所定の関係をもって一つのファイルとして設定する手段であるものとすることもできる。こうすれば、新規な書類を指定してデジタル署名をすることができる。

【0011】さらに、本発明のデジタル多重署名装置において、前記一覧表示手段により表示された関係に含まれる書類を指定したとき、該指定された書類を表示する書類表示手段を備えるものとすることもできる。

【0012】あるいは、本発明のデジタル多重署名装置において、前記署名追加手段は、前記新たなデジタル署名の追加と共に該デジタル署名に対する検証用データを有する書類を追加する手段であり、前記ファイル設定手段は、前記追加されたデジタル署名および前記追加された書類と前記指定されたファイルに含まれる書類およびデジタル署名と所定の関係をもって一つのファイルとして設定する手段であるものとすることもできる。こうすれば、正当なデジタル署名を証明することができる。この態様の本発明のデジタル多重署名装置において、前記書類は該書類の追加と共に追加されたデジタル署名に対する検証用書類を含み、前記ファイル解析手段は前記検証用書類に基づいて該検証用書類を含む書類の追加と共に追加されたデジタル署名を検証する署名検証手段を備

えるものとすることもできる。こうすれば、ファイルに含まれるデジタル署名が正当なものであるかを判定することができる。

【0013】本発明の記憶媒体は、指定されたファイルに含まれる書類とデジタル署名との関係を解析するファイル解析処理と、該解析された関係を一覧表示する一覧表示処理と、該一覧表示された関係に対して新たなデジタル署名を追加可能な署名追加処理と、該新たなデジタル署名が追加されたとき、該追加されたデジタル署名と前記指定されたファイルに含まれる書類およびデジタル署名とを所定の関係をもって一つのファイルとして設定するファイル設定処理とをコンピュータに実行させるためのプログラムをコンピュータに読み取り可能に記憶したことを要旨とする。

【0014】この本発明の記憶媒体では、コンピュータを前述の本発明のデジタル多重署名装置として動作させることができる。即ち、コンピュータにこの記憶媒体に記憶されたプログラムを読み取らせ、読み込んだプログラムを実行させることにより、コンピュータを、ファイル解析処理によって解析した指定されたファイルに含まれる書類とデジタル署名との関係を一覧表示する一覧表示処理に基づくファイルに含まれる書類とデジタル署名とを容易に確認することができるという効果や、一覧表示された関係に対して新たなデジタル署名を追加する署名追加処理に基づく簡易に新たなデジタル署名を追加することができるという効果を奏するデジタル多重署名装置として動作させることができる。

【0015】

【発明の実施の形態】次に、本発明の実施の形態を実施例を用いて説明する。図1は本発明の一実施例であるデジタル多重署名装置5の構成の概略を示す構成図であり、図2はこのデジタル多重署名装置5が実現されるコンピュータ10の構成の概略を示す構成図である。まず、説明の都合上、図2に従って実施例のデジタル多重署名装置5が実現されるコンピュータ10の構成について説明する。

【0016】図2に示すように、このコンピュータ10は、プロセッサバス22に接続された演算処理部20、プロセッサバス22をローカルバス32（例えば、PCIバス）に接続するバスブリッジ30、ローカルバス32を介して演算処理部20のCPU21等によりアクセスを受けるコントローラ部40、各種のI/O装置等を制御する機器が低速の外部バス42（例えば、ISAバス）に接続されたI/O部60、および周辺機器であるキーボード72、スピーカ74、カラーCRT76などから構成されている。

【0017】演算処理部20は、中央演算処理装置としてのCPU21（本実施例ではインテル社製Pentiumを使用）、キャッシュメモリ23、そのキャッシュコントローラ24およびメインメモリ25から構成され

ている。バスブリッジ30は、プロセッサバス22とローカルバス32との間でデータ伝送を制御するコントローラである。CPU21は、メモリ管理ユニット（MMU）を内蔵し、実際の物理アドレスより広い論理アドレスにアクセスすることができる。

【0018】コントローラ部40は、モニタ（カラーCRT）76への画像の表示を司るグラフィックスコントローラ（以下、CRTCと呼ぶ）44、接続されるSCSI機器とのデータ転送を司るSCSIコントローラ46、ローカルバス32と外部バス42との間でデータ伝送を制御するバスブリッジ48から構成されている。CRTC44は、カラーCRT76に対して640×480ドット、16万色表示が可能である。なお、表示用のフォントを記憶したキャラクタジェネレータや所定のコマンドを受け取って所定の図形を描画するグラフィックコントローラ、更には描画画像を記憶するビデオメモリ等は、このCRTC44に実装されているが、これらの構成は周知のものであるので、図2では図示を省略した。

【0019】バスブリッジ48を介して接続された外部バス42は、各種のI/O機器が接続される入出力制御用のバスであり、DMAコントローラ（以下単にDMACと呼ぶ）50、リアルタイムクロック（RTC）52、複合I/Oポート54、サウンドI/O56、キーボード72および2ボタンマウス73とのインタフェースを司るキーボードインタフェース（以下KEYと呼ぶ）64、優先順位を有する割り込み制御を行なう割り込みコントローラ（以下PICと呼ぶ）66、各種の時間カウントやビープ音を発生するタイマ68などから構成されている。外部バス42には、各種拡張ボードを実装可能なISAスロット62が接続されている。

【0020】複合I/Oポート54には、パラレル出力やシリアル出力の他にフロッピディスク装置82やハードディスク84を制御する信号を入出力するポートが用意されている。また、パラレル入出力にはパラレルポート86を介してプリンタ88が接続されており、シリアル入出力にはシリアルポート90を介してモデム92が接続されている。また、サウンドI/O56には、上述したスピーカ74の他にマイクロフォン96が接続可能とされている。

【0021】このコンピュータ10のハードディスク84には、種々のデバイスドライバが記憶されており、コンピュータ10は立ち上げ時にハードディスク84から必要なデバイスドライバを読み込んで組み込む。デバイスドライバとしては、複合I/Oポート54を介してのプリンタ88への印字を可能にするプリンタドライバなどがある。

【0022】ハードディスク84には、「WINDOW S NT」というGUIを備えたオペレーティングシステムが記憶されており（「WINDOWS NT」はマイクロソフト社の商標）、コンピュータ10は、このオ

ペレーティングシステムを読み込み、その後アプリケーションプログラムをこのオペレーティングシステム上で動作するよう主記憶上に読み込んで実行する。

【0023】次に、図1に従って実施例のデジタル多重署名装置5について説明する。このデジタル多重署名装置5は、上述したコンピュータ10において、そのハードウェアとソフトウェアが一体となって実現されるものであり、図1はソフトウェアにより実現される部分も含めてその機能をブロック図として表わしたものである。

【0024】デジタル多重署名装置5は、指定された所定の構造のファイルをハードディスク84などから読み込んでそのファイルに含まれる書類やデジタル署名等を解析するファイル解析部FAと、ファイル解析部FAにより解析されたファイルに含まれる書類やデジタル署名などを解析された関係に基づいてカラーCRT76に一覧表示する一覧表示部DFと、ファイル解析部FAにより解析されたファイルに新たなデジタル署名の追加を行なう署名追加部ASと、書類を指定してデジタル署名を行なう書類指定署名部ISと、署名追加部ASによりデジタル署名が追加されたときや書類指定署名部ISにより新規に書類が指定されてデジタル署名がなされたときにそれらのすべてを所定の階層構造の一つのファイルに設定するファイル設定部FSとを備える。

【0025】ファイル解析部FAは、ファイルの解析の際にそのファイルに含まれるデジタル署名の正当性を検証する署名検証部CSを備えている。また、署名追加部ASは、デジタル署名を追加する際の一覧表示部DFにより一覧表示された関係に追加されるデジタル署名の欄をその一覧表内に表示する追加署名欄表示部ADSと、デジタル署名の追加に先立って書類の追加を行なう際の一覧表示部DFにより一覧表示された関係に追加される書類の欄をその一覧表内に表示する追加書類欄表示部ADPとを備える。

【0026】これらの各機能ブロックは、前述したようにコンピュータ10のハードウェアと後述するソフトウェアとが一体となって実現されるものであり、例えば、ファイル解析部FAは、ハードウェアとしては演算処理部20に含まれる各部の他、プロセッサバス22やバスブリッジ30、ローカルバス32、バスブリッジ48を介して接続される複合I/Oポート54に接続されたハードディスク84やフロッピディスク装置82、同じく外部バス42を介して接続されたKEY64に接続されたキーボード72や2ボタンマウス73などが該当し、ソフトウェアとしては後述する図3に例示するデジタル多重署名ダイアログ表示ルーチンのステップS102の処理として行なわれる図13に例示するファイル解析処理ルーチンなどが該当する。また、一覧表示部DFは、ハードウェアとしては演算処理部20に含まれる各部の他、プロセッサバス22やバスブリッジ30、ローカルバス32を介して接続されるグラフィックスコントロー

ラ44が該当し、ソフトウェアとしては図3に例示するデジタル多重署名ダイアログ表示ルーチンのステップS104の処理などが該当する。署名追加部ASは、ハードウェアとしては同じく演算処理部20に含まれる各部の他、プロセッサバス22やバスブリッジ30、ローカルバス32、バスブリッジ48を介して接続されるKEY64に接続されたキーボード72や2ボタンマウス73、同じくバスブリッジ48を介して接続される複合I/Oポート54のハードディスク84やフロッピディスク装置82などが該当し、ソフトウェアとしては後述する図5に例示する本文指定処理ルーチンや図7に例示する添付資料指定処理ルーチン、図9に例示するデジタル署名処理ルーチンなどが該当する。ファイル設定部FSは、ハードウェアとして同じく演算処理部20に含まれる各部の他、プロセッサバス22やバスブリッジ30、ローカルバス32、バスブリッジ48を介して接続される複合I/Oポート54に接続されたフロッピディスク装置82やハードディスク84などが該当し、ソフトウェアとしては図9に例示するデジタル署名処理ルーチンのステップS138の処理などが該当する。書類指定署名部ISは、署名追加部ASと同様に、ハードウェアとしては演算処理部20に含まれる各部の他、プロセッサバス22やバスブリッジ30、ローカルバス32、バスブリッジ48を介して接続されるKEY64に接続されたキーボード72や2ボタンマウス73、同じくバスブリッジ48を介して接続される複合I/Oポート54のハードディスク84やフロッピディスク装置82などが該当し、ソフトウェアとしては後述する図5に例示する本文指定処理ルーチンや図7に例示する添付資料指定処理ルーチン、図9に例示するデジタル署名処理ルーチンなどが該当する。

【0027】次にこうして構成された実施例のデジタル多重署名装置5の動作について説明する。図3は、コンピュータ10がデジタル多重署名装置5として起動されたときに起動されるデジタル多重署名ダイアログ表示ルーチンの一例を示すフローチャートである。このルーチンが起動されると、CPU21は、まず、デジタル多重署名装置5の起動と同時にファイルの指定がなされていたか否かの判定を行なう処理を実行する(ステップS100)。コンピュータ10をデジタル多重署名装置5として起動する際にファイルを指定して起動したときには、ファイルの指定ありと判定して、ファイルの解析処理を実行して(ステップS102)、解析結果に基づいてデジタル多重署名ダイアログDDを表示する(ステップS104)。ステップS102のファイルの解析処理および解析結果に基づいてデジタル多重署名ダイアログDDを表示する処理については後述する。

【0028】一方、コンピュータ10をデジタル多重署名装置5として起動する際にファイルを指定しなかったときには、ファイルの指定なしと判定してデジタル多重署

名ダイアログDDを表示して(ステップS104)、本ルーチンを終了する。デジタル多重署名ダイアログDDの一例を図4に示す。図示するように、デジタル多重署名ダイアログDDには、デジタル署名の階層を示す署名レベルやデジタル署名の署名者名、デジタル署名の検証結果が表示される検証結果、デジタル署名の対象となる本文や添付書類の名称を表示するファイル名の表示欄が設けられている。いま、ファイルを指定しなかった場合を考えているから、それらの欄には何も表示されていない。また、デジタル多重署名ダイアログDDには、これからデジタル署名を行なうために必要なコマンドがメニューとして表示され、これらのメニューを2ボタンマウス73でクリックしたりキーボード72から入力することにより各コマンドを実行できるようになっている。メニューに含まれるコマンドとしては、デジタル署名を行なう対象としての申請書などの本文を指定するための本文指定コマンド、本文に添付すべき資料を指定するための添付資料指定コマンド、デジタル多重署名ダイアログDDに表示された内容に対してデジタル署名を行なうためのデジタル署名コマンドなどがある。

【0029】こうしたデジタル多重署名ダイアログDDのメニューから本文指定コマンドをキーボード72から入力したり2ボタンマウス73をクリックしたときには、図5に例示する本文指定処理ルーチンが起動される。本ルーチンが起動されると、CPU21は、まずハードディスク84の予め指定されたディレクトリに記憶されたファイルを新たなウインドウを開いて一覧表示する処理を実行する(ステップS110)。このファイルの一覧表示は図示しないが所定の大きさのウインドウが開かれてファイル名が規則正しく整列して表示されるものであれば如何なるものでもかまわない。次に、こうして一覧表示したものから操作者が本文ファイルをキーボード72からの入力や2ボタンマウス73によるクリックで選択すると(ステップS112)、デジタル多重署名ダイアログDDに表示欄Rnが表示されると共に(ステップS114)、選択した本文のファイル名を「ファイル名」の欄に表示して(ステップS116)、本ルーチンを終了する。本文として「申請書」を選択したときに本文が表示欄R1に表示された状態のデジタル多重署名ダイアログDDを図6に示す。このとき、まだデジタル署名はなされていないから、「ファイル名」の欄にのみその内容が表示される。

【0030】本文に対して添付資料がある場合には、本文の指定を行ってから、デジタル多重署名ダイアログDDのメニューから添付資料指定コマンドをキーボード72や2ボタンマウス73から入力する。この添付資料指定コマンドが入力されたときに実行される添付資料指定処理ルーチンを図7に例示する。本ルーチンが起動されると、CPU21は、本文指定処理ルーチンの際と同様に、まずハードディスク84の予め指定されたディレ

クトリに記憶されたファイルを新たなウインドウを開いて一覧表示する処理を実行する(ステップS120)。そして、一覧表示されたものから操作者が添付資料ファイルをキーボード72や2ボタンマウス73から入力することにより選択すると(ステップS122)、デジタル多重署名ダイアログDDの「ファイル名」の本文が表示された欄の下に追加欄が表示されると共に(ステップS124)、選択した添付資料のファイル名を追加された欄に表示して(ステップS126)、本ルーチンを終了する。添付資料として「補足資料」を選択したときに添付資料本が追加欄に表示された状態のデジタル多重署名ダイアログDDを図8に示す。こうした添付資料の指定は繰り返し行なうことができ、その指定毎に追加欄が表示されて添付資料のファイル名が表示される。

【0031】本文の指定後は、メニューのデジタル署名コマンドを入力することにより、この本文に対して、添付資料があるときにはその添付資料を含めたすべての書類に対してデジタル署名を行なうことができる。図9は、デジタル署名コマンドが入力されたときにデジタル多重署名装置5により実行されるデジタル署名処理ルーチンの一例を示すフローチャートである。このルーチンが実行されると、CPU21は、まずデジタル署名の署名者の名前を「署名者名」の欄に表示し(ステップS130)、デジタル署名の権限確認の処理を実行する(ステップS132)。デジタル署名の権限確認は、秘密鍵パスワードの入力を要請するパスワード入力画面を開いてパスワードを入力させ、これを予め登録されているパスワードと比較することなどにより行なうことができる。こうしたデジタル署名の権限確認の結果を判定し(ステップS134)、正当な者であると判定すると、指定した本文や添付資料のすべてのファイルのハッシュ値を計算して署名情報としてファイル化すると共に(ステップS136)、署名レベルと検証結果を正しいものとして表示し(ステップS138)、指定した本文や添付資料、署名情報、デジタル署名の認定書、デジタル署名を一つのファイルとして設定して(ステップS139)、本ルーチンを終了する。検証結果が正当な者と判定された後に表示されるデジタル多重署名ダイアログDDの一例を図10に示し、設定されるファイルの構造を模式的に例示する模式図を図11に示す。一方、権限確認結果として正当な者と判定されなかったときには、直ちに本ルーチンは終了する。

【0032】これまではコンピュータ10をデジタル多重署名装置5として起動する際にファイルを指定しなかったときの処理について説明したが、次にコンピュータ10をデジタル多重署名装置5として起動する際にファイルを指定したときの処理について説明する。いま、指定したファイルの構造として図12に例示するファイルF2であったとする。このファイルF2は、前述したファイルを指定しなかったときの処理によりAによりデジ



タル署名されて設定されたファイルF1に、Bが本文として「回答」を追加すると共に添付資料として「回答補足」を追加し、これらすべてに対してデジタル署名して全体を一つのファイルとして設定されたものである。この場合、図3のデジタル多重署名ダイアログ表示ルーチンでは、ステップS100でファイルの指定ありと判定して、ファイルの解析処理を実行し（ステップS102）、解析結果に基づいてデジタル多重署名ダイアログDDを表示する（ステップS104）。

【0033】ファイルの解析処理は図13に例示するファイル解析処理ルーチンにより行なわれる。本ルーチンが実行されると、CPU21は、まずカウンタNに初期値としての値0を設定する処理を実行する（ステップS140）。続いて、カウンタNをインクリメントし（ステップS142）、カウンタNの値に基づいてハードディスク84の所定ディレクトリ内にディレクトリを設定する（ステップS144）。実施例では、ディレクトリ名として「Level」にカウンタNの値を文字として付加したものがハードディスク84に作成されることになる。そして、ファイルのカウンタNの値の階層の本文や添付資料、署名情報、認定書、その階より下位の多重署名済ファイルに対してそれぞれ一時ファイルを設定したディレクトリに作成する（ステップS146）。図12のファイルF2の例では、本文として「回答」、添付資料として「回答補足」、デジタル署名Bの認定書、デジタル署名Bを行なったときに図9のデジタル署名処理ルーチンのステップS136の処理で作成された署名情報、下位の多重署名済ファイルとして図12中のファイルF1がそれぞれ一時ファイルとしてハードディスク84のディレクトリ「Level1」に作成されるのである。

【0034】次に、デジタル署名の検証の処理を実行する（ステップS148）。デジタル署名の検証は、ファイル全体のハッシュ値を計算し、計算したハッシュ値と署名情報として記載されているハッシュ値とを比較することにより行なわれる。そして、検証結果を一時ファイルとして同一のディレクトリに格納する（ステップS150）。図14にディレクトリ「Level1」に格納される一時ファイルの内容を模式的に示す。

【0035】次に、下位の多重署名済ファイルがあるかを判定する処理を実行する（ステップS152）。図12の例では、下位の多重署名済ファイルとしてファイルF1があるから、下位の多重署名済ファイルがあると判定されて、ステップS142の処理に戻る。ステップS142ではカウンタNがインクリメントされるから、カウンタNの値の階層、すなわち図12のファイル構造におけるファイルF1について同様にステップS144ないしS152の処理が実行されてディレクトリ「Level2」に一時ファイルが作成される。ただし、ファイルF1には下位の多重署名済ファイルは存在しないか

ら、ステップS146の処理ではこの下位の多重署名済ファイルの一時ファイルは作成されない。

【0036】ステップS152で下位の多重署名済ファイルがないと判定されると、図13のファイル解析処理ルーチンは終了し、図3のデジタル多重署名ダイアログ表示ルーチンに戻り、ステップS104のデジタル多重署名ダイアログDDの表示処理を行なう。このデジタル多重署名ダイアログDDの表示処理は、図13のファイル解析処理ルーチンにより作成された各ディレクトリと各ディレクトリ内に作成された一時ファイルに基づいて行なわれる。すなわち、表示欄R2が表示され、ディレクトリ名の用いられたカウンタNの値に基づいて作成されたディレクトリの数から降順の数が「署名レベル」の欄に、そのディレクトリに作成された一時ファイルのうち認定書に記載されたデジタル署名の名前が「署名者名」の欄に、同じく検証結果の内容が「検証結果」の欄に、本文や添付資料のファイル名がそれぞれ「ファイル名」の欄に、それぞれ表示される。この際、2以上のディレクトリが作成されているときには、その下に表示欄R1が表示され、同様に各欄が表示される。図12のファイル構造をデジタル多重署名ダイアログDDに表示したときの一例を図15に示す。

【0037】こうしたコンピュータ10をデジタル多重署名装置5として起動する際にファイルを指定したときの処理でも、デジタル多重署名ダイアログDDのメニューの本文指定コマンドや添付資料指定コマンド、デジタル署名コマンドを入力することにより、図5に例示する本文指定処理ルーチンや図7に例示する添付資料指定処理ルーチン、図9に例示するデジタル署名処理ルーチンを実行することができる。図12のファイル構造に対してこれらのコマンドを実行したときの様子について簡単に説明する。なお、各処理の詳細は前述した。

【0038】デジタル多重署名ダイアログDDの本文指定コマンドが入力されると、図5に例示する本文指定処理ルーチンが起動され、操作者がステップS112の処理で本文として「確認」のファイルを選択すると、図16に例示するデジタル多重署名ダイアログDDのように表示欄R3が追加されて（ステップS114）、その表示欄R3の「ファイル名」の欄に本文のファイル名として「確認」が表示される（ステップS116）。

【0039】デジタル多重署名ダイアログDDの添付資料指定コマンドが入力されると、図7に例示する添付資料指定処理ルーチンが起動され、操作者がステップS122の処理で添付資料として「確認補足」のファイルを選択すると、図17に例示するデジタル多重署名ダイアログDDの表示欄R3に「ファイル名」の本文の表示欄として「確認」が表示された欄の下に追加欄が追加される（ステップS124）、この追加欄に添付資料のファイル名として「確認補足」が表示される（ステップS126）。

【0040】デジタル多重署名ダイアログDDのデジタル署名コマンドが入力されると、図9に例示するデジタル署名処理ルーチンが起動され、デジタル署名の署名者の名前を「署名者名」の欄に表示し（ステップS130）、デジタル署名を権限確認して（ステップS132）、デジタル署名の権限確認の結果を判定する（ステップS134）。そして、正当な者であると判定すると、署名情報を作成して（ステップS136）、署名レベルと検証結果を正しいものとして表示し（ステップS138）、指定した本文や添付資料、署名情報、デジタル署名の認定書、デジタル署名を一つのファイルとして設定する（ステップS139）。権限確認結果が正当な者と判定された後に表示されるデジタル多重署名ダイアログDDの一例を図18に示し、設定されるファイルの構造を模式的に例示する模式図を図19に示す。

【0041】こうして表示されたデジタル多重署名ダイアログDDは、デジタル多重署名ダイアログDDが表示されているすべての段階で、各欄の「ファイル名」に表示された本文や添付資料をキーボード72や2ボタンマウス73により入力すると、該当する本文や添付資料が、それを作成したアプリケーションの起動を伴って表示されるようになっている。例えば、ファイル解析を行なったすぐ後に表示される図15の状態やデジタル署名が行なわれた後に表示される図10や図18の状態のときにおけるデジタル多重署名ダイアログDDの「ファイル名」に表示された本文や添付資料への入力に基づく本文や添付資料のアプリケーションを伴っての表示は勿論、本文を指定した直後の図6や図8の状態や添付資料を指定した直後の図16や図17の状態のときにおいてもデジタル多重署名ダイアログDDの「ファイル名」に表示された本文や添付資料への入力に基づく本文や添付資料のアプリケーションを伴っての表示も行なわれる。こうした文書をアプリケーションの起動を伴って表示する処理の詳細は周知であるから、これ以上の説明は省略する。

【0042】以上説明した実施例のデジタル多重署名装置5によれば、複数のデジタル署名を含むファイルを解析してそのレベル毎に分けて一覧表示するから、ファイルのデジタル多重署名の状態を一目で理解することができる。しかも、一覧表示された本文や添付書類を直ちに開いて確認することができる。また、一覧表示された内容を確認しながら本文の追加や添付資料の追加、全体に対してのデジタル署名を行なうことができる。

【0043】また、実施例のデジタル多重署名装置5によれば、デジタル署名の正当性を判定することができる。この結果、契約書などの重要書類に対して使用することもできる。さらに、実施例のデジタル多重署名装置5によれば、新規に本文を指定してデジタル署名することもできる。

【0044】実施例のデジタル多重署名装置5では、デ

ジタル署名の検証を行なうものとしたが、デジタル署名の検証を行なわないものとしても差し支えない。また、実施例のデジタル多重署名装置5では、デジタル多重署名ダイアログDDに表示されたファイル名を2ボタンマウス73などでクリックすることにより、本文や添付資料を作成したアプリケーションの起動を伴って本文や添付資料を表示するものとしたが、こうした機能のないものとしてもかまわない。実施例のデジタル多重署名装置5では、「WINDOWS NT」というオペレーティングシステム上で動作するものとしたが、その他の如何なるオペレーションシステム上で動作するものとしてもよい。

【0045】実施例のデジタル多重署名装置5では、ハードウェアとしてのコンピュータ10と、コンピュータ10をデジタル多重署名装置5として機能させるソフトウェアとが一体のものとして説明したが、コンピュータ10を上記した実施例のデジタル多重署名装置5として機能させるプログラムをコンピュータ10が読みとり可能に記憶した記憶媒体、例えば、フロッピディスクやCD-ROM、DVDなどとしてもよい。これらの記憶媒体は、コンピュータ10に読み込ませることによりコンピュータ10が実施例のデジタル多重署名装置5として機能するからである。

【0046】以上、本発明の実施の形態について実施例を用いて説明したが、本発明はこうした実施例に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内において、種々なる形態で実施し得ることは勿論である。

#### 【図面の簡単な説明】

【図1】 本発明の一実施例であるデジタル多重署名装置5の構成の概略を示す構成図である。

【図2】 実施例のデジタル多重署名装置5が実現されるコンピュータ10の構成の概略を示す構成図である。

【図3】 コンピュータ10がデジタル多重署名装置5として起動されたときに起動されるデジタル多重署名ダイアログ表示ルーチンの一例を示すフローチャートである。

【図4】 カラーCRT76に表示されるデジタル多重署名ダイアログDDの一例を示す説明図である。

【図5】 本文指定コマンドが入力されたときにデジタル多重署名装置5により実行される本文指定処理ルーチンの一例を示すフローチャートである。

【図6】 表示欄R1を表示した際のデジタル多重署名ダイアログDDを例示する説明図である。

【図7】 添付資料指定コマンドが入力されたときデジタル多重署名装置5により実行される添付資料指定処理ルーチンの一例を示すフローチャートである。

【図8】 添付資料の追加欄に添付資料を表示した際のデジタル多重署名ダイアログDDを例示する説明図である。

【図9】 デジタル署名コマンドが入力されたときにデジタル多重署名装置5により実行されるデジタル署名処理ルーチンの一例を示すフローチャートである。

【図10】 デジタル署名がなされてフィルの設定がなされたときのデジタル多重署名ダイアログDDを例示する説明図である。

【図11】 ファイルが設定されたときのファイルの構造を模式的に例示する説明図である。

【図12】 指定されたファイルF2の構造を模式的に例示する説明図である。

【図13】 デジタル多重署名装置5により実行されるファイル解析処理ルーチンの一例を示すフローチャートである。

【図14】 ディレクトリ「Level1」に格納される一時ファイルの内容を模式的に例示する説明図である。

【図15】 図12のファイル構造をデジタル多重署名ダイアログDDに表示したときの一例を示す説明図である。

【図16】 表示欄R3を表示した際のデジタル多重署名ダイアログDDを例示する説明図である。

【図17】 添付資料の追加欄に添付資料を表示した際のデジタル多重署名ダイアログDDを例示する説明図である。

【図18】 デジタル署名がなされてフィルの設定がな

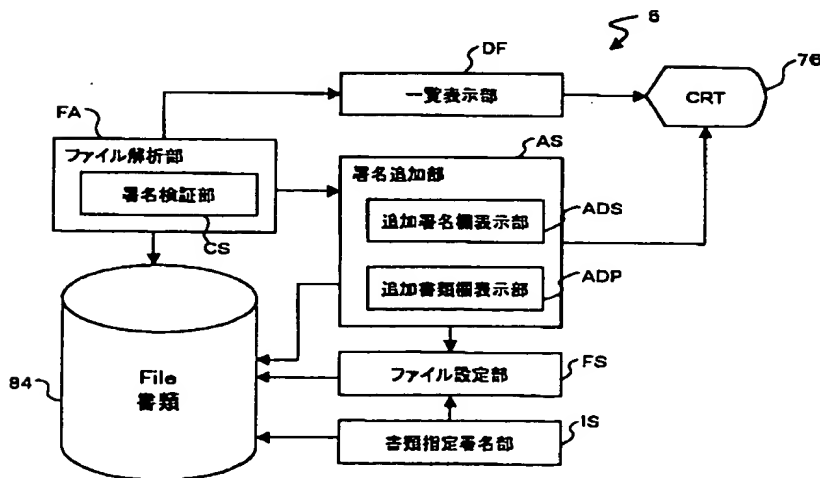
されたときのデジタル多重署名ダイアログDDを例示する説明図である。

【図19】 ファイルが設定されたときのファイルの構造を模式的に例示する説明図である。

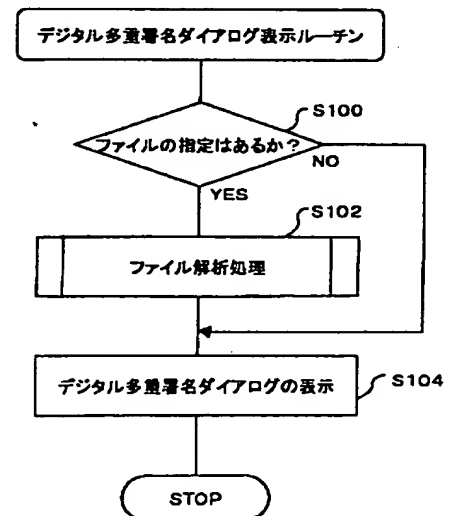
【符号の説明】

5 デジタル多重署名装置、10 コンピュータ、20 演算処理部、21 CPU、22 プロセッサバス、23 キャッシュメモリ、24 キャッシュコントローラ、25 メインメモリ、30 バスブリッジ、32 ローカルバス、40 コントローラ部、42 外部バス、44 グラフィックスコントローラ、46 SCSIコントローラ、48 バスブリッジ、50 DMA C、52 リアルタイムクロック、54 複合I/Oポート、56 サウンドI/O、60 I/O部、62 ISAスロット、64 キーボードインタフェース、66 割り込みコントローラ、68 タイマ、72 キーボード、73 2ボタンマウス、74 スピーカ、76 カラーCRT、82 フロッピディスク装置、84ハードディスク、86 パラレルポート、88 プリンタ、90 シリアルポート、92 モデム、96 マイクロフォン、FA ファイル解析部、CS 署名検証部、DF 一覧表示部、AS 署名追加部、ADS 追加署名欄表示部、ADP 追加書類欄表示部、FS ファイル設定部、IS 書類指定署名部。

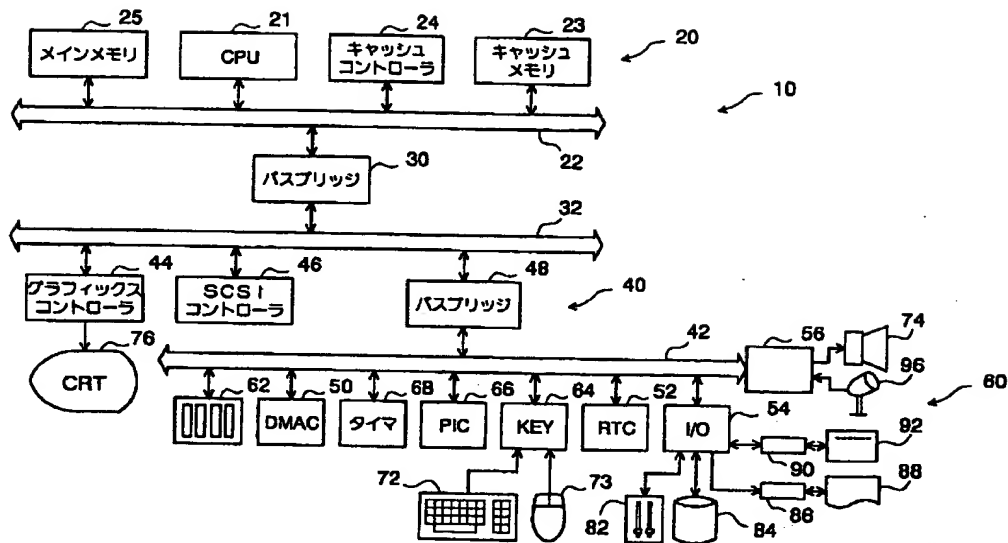
【図1】



【図3】



【図2】



【図4】

DD

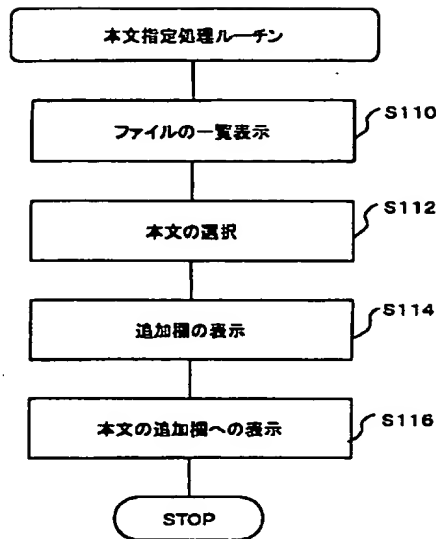
Figure 4 shows a screenshot of a software window titled "Form2". The window has a menu bar with "本文指定", "添付資料指定", and "デジタル署名". Below the menu bar is a table with the following headers: "署名レベル", "署名者名", "検証結果", and "ファイル名". The table is currently empty.

【図6】

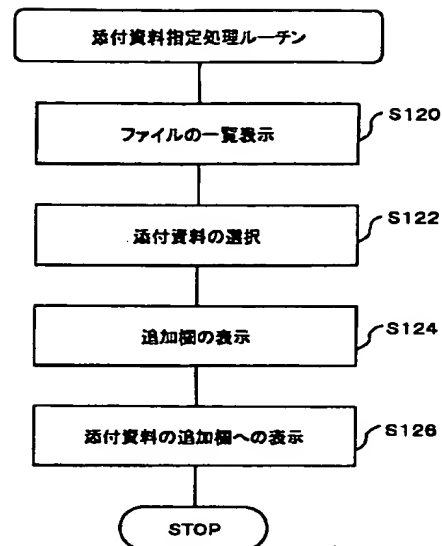
DD

Figure 6 shows a screenshot of a software window titled "Form1". The window has a menu bar with "本文指定", "添付資料指定", and "デジタル署名". Below the menu bar is a table with the following headers: "署名レベル", "署名者名", "検証結果", and "ファイル名". The table contains three data rows. The first row has values "0", "0", "0", and "申請書.txt". The second and third rows are partially visible but their content is not fully legible.

【図5】



【図7】



【図8】

Form1

本文指定 添付資料指定 エンタール署名

署名レベル	署名者名	使用結果	ファイル名
①	②	③	申請書.txt
			補足資料1.txt

DD

【図10】

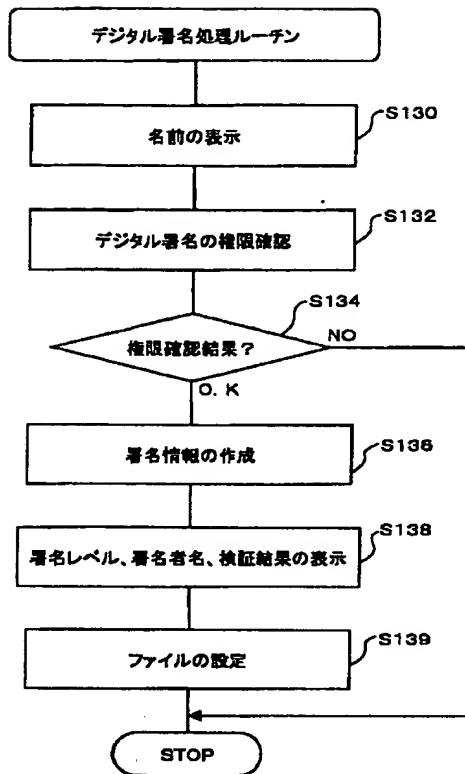
Form1

本文指定 添付資料指定 エンタール署名

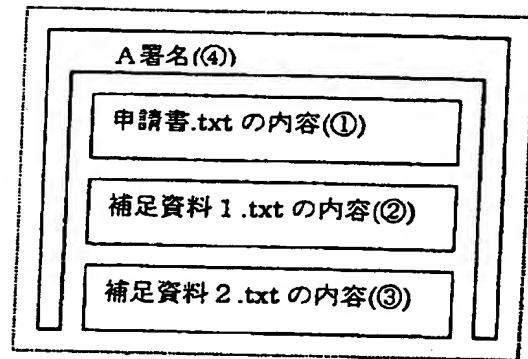
署名レベル	署名者名	使用結果	ファイル名
①	②	③	申請書.txt
			補足資料1.txt
			補足資料2.txt

DD

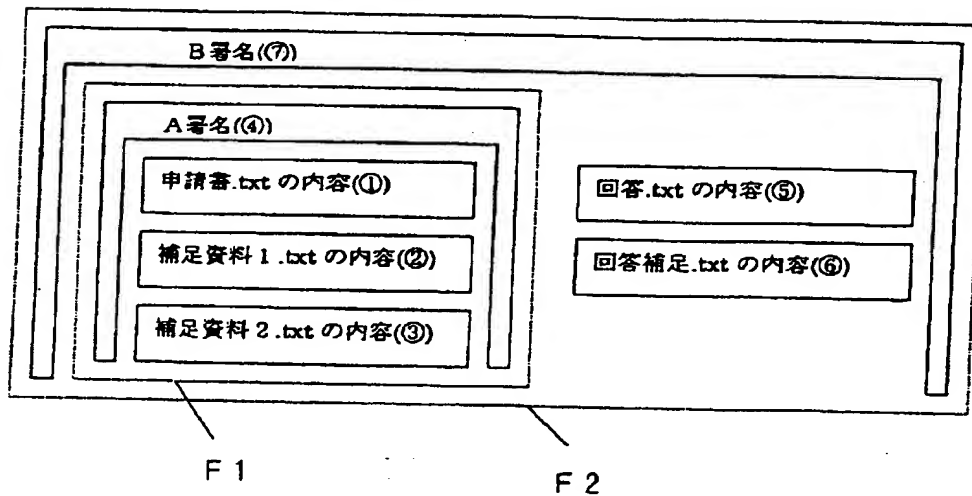
【図9】



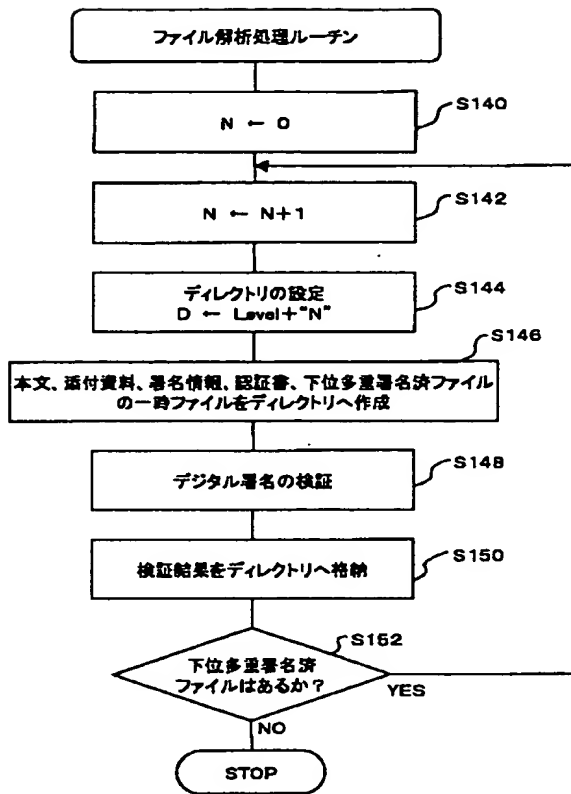
【図11】



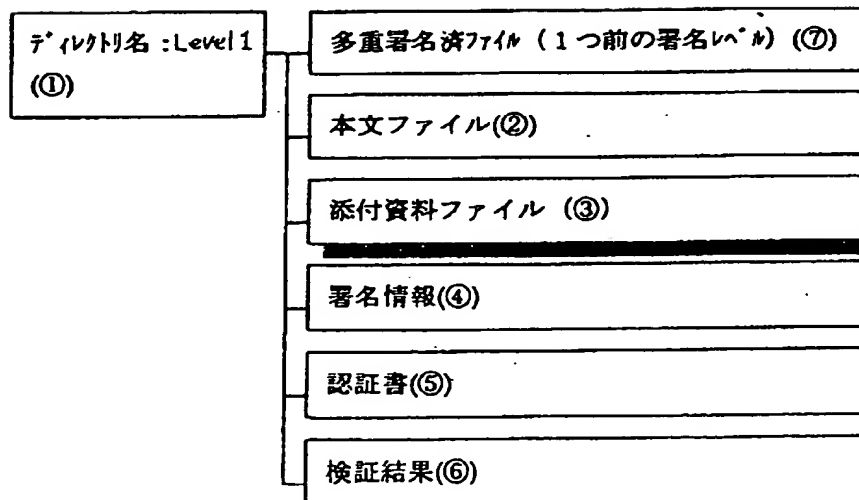
【図12】



【図13】



【図14】



【図15】

DD

署名レベル	署名者名	検索結果	ファイル名
2	B	O	回答.txt
2	B	O	回答補足.txt
1	A	O	申請書.txt
			補足資料1.txt
			補足資料2.txt

【図16】

DD

署名レベル	署名者名	検索結果	ファイル名
1	A	O	回答.txt
2	B	O	回答.txt
1	A	O	申請書.txt
			補足資料1.txt
			補足資料2.txt



【図17】

DD

氏名レベル	氏名番号	性別	ファイル名
3	C	O	満足.txt 満足満足.txt
2	B	O	回答.txt 回答満足.txt
1	A	O	申請書.txt 満足資料1.txt 満足資料2.txt

【図18】

DD

氏名レベル	氏名番号	性別	ファイル名
3	C	O	満足.txt 満足満足.txt
2	B	O	回答.txt 回答満足.txt
1	A	O	申請書.txt 満足資料1.txt 満足資料2.txt

【図19】

